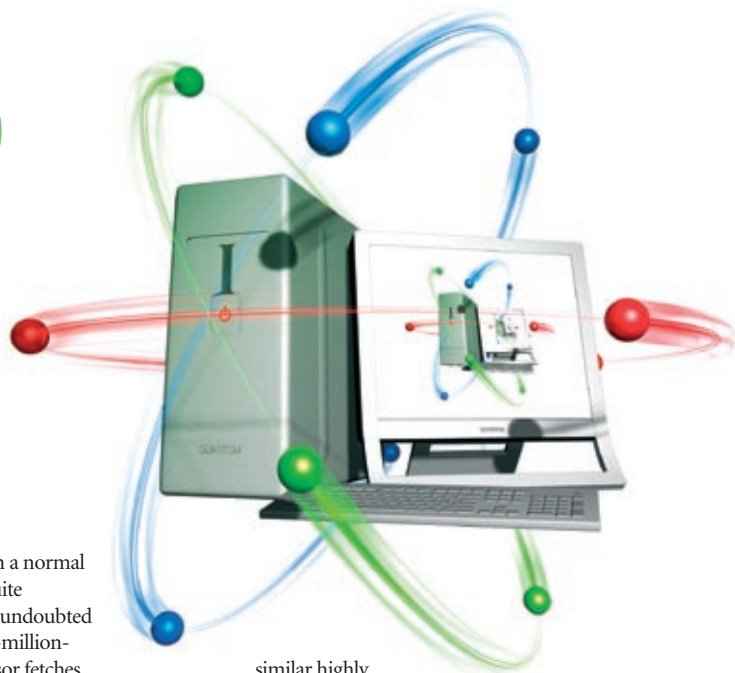




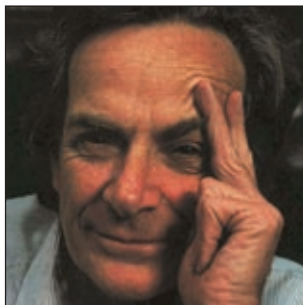
Quantum Leaps

Quantum computing may be difficult to understand, but it's not so hard to appreciate the phenomenal power it could provide. **Jon Thompson** considers how future applications could benefit from a leap of faith



For more than 20 years pundits and scientists have predicted the development of quantum computers, which would harness the mysterious world of quantum mechanics to produce computers with immense computational power, way beyond what's currently possible. The theories behind them seem outlandish, but early experiments suggest that they might be accurate.

How far are we from building a computer that exploits quantum theory's massive potential? Accepted wisdom has dictated that practical problems and limitations mean a working device is many decades away, but recent breakthroughs have led some research teams to put it as soon as 2007. What can we reasonably expect? And will anyone outside of quantum physics ever understand the baffling way these devices are designed to work?



"I think I can safely say that nobody understands quantum mechanics." Winner of the 1965 Nobel Prize for Physics and father of the quantum computer, Professor Richard Feynman

WORLDS AWAY

The basic principle by which a normal computer works remains quite straightforward, despite the undoubted complexity of today's multi-million-transistor chips. The processor fetches data and instructions from RAM or ROM. Each instruction causes the processing of data by complex configurations of logic gates that implement various arithmetic and other operations. Some, for instance, take decisions about what to do next based on the results of previous calculations. In various forms, this process underlies all modern computing. But things aren't quite the same in quantum computers.

The first difference is in how a quantum computer represents single bits of data within the processor and in RAM. Current research uses qubits (also known as qubits), which can be anything from a single molecule to an atom, or even an electron.

To represent a binary one or zero, the computer uses a pair of lasers or

similar highly focused energy sources to make individual qubits spin in one of two directions, called up and down. The processor uses logic gates also based on atomic particles, which observe the state of the qubits to produce results and take decisions.

At least in this way, quantum computers seem to operate similarly to everyday hardware, but from here on in quantum computers part company with convention. How they generate overwhelming computational power seems, at first, impossible. Even how it all works is still open to interpretation and debate, despite experiments proving that the bizarre theory does in fact reflect reality.

This is because qubits can do something that should be impossible. Put simply, they can spin in both directions at once. Quantum physicists call this strange ability superposition. To put a qubit into superposition, one energy source sets it spinning in one direction. Another then blasts it to make it

A BRIEF HISTORY OF SILICON

The idea of putting several transistors on a single chip originally came from a Royal Radar Establishment engineer called Geoffrey Dummer in 1952. Unfortunately for him, technical difficulties meant that Jack Kilby of Texas Instruments became the first to patent a working Solid Circuit in 1959.

The first commercial chips (correctly known as integrated circuits, or ICs) contained a few dozen interconnected transistors. At the time, newly developing missile and space technologies

required fast, cheap and small transistors, and prefabricated ICs were ideal. As a result, projects such as that to build the flight computer used on the Apollo missions consumed much of the available supply of ICs in the early 1960s.

Over the decade, as manufacturing practices developed, the transistor count rose steadily, roughly in line with Moore's Law. Intel founder Gordon Moore wrote in *Electronics* magazine in 1965 that the number of transistors on a single chip would probably continue to double about

every 18 months or so, a rule that is only just beginning to encounter difficulties as we reach the physical limits of silicon.

By 1970, the world's first microprocessor, the four-bit Intel 4004, carried 2,300 transistors. A year later, its successor, the eight-bit 8008, managed to squeeze in 3,300. Microprocessors of all descriptions quickly became widespread during the early 1970s, fuelled by the public's desire for digital watches, calculators and other electronic items, and the need to build faster computers. By the 1980s, Very Large Scale Integration (VLSI) chip fabrication techniques had pushed the transistor count to around a million per chip. By 1986, the



spin the opposite way, but using only half the power of the first.

That's not the only strange thing. Being in two states at once means that a register made of several qubits represents all its possible values at once. If a quantum register had eight qubits, for example, it would represent 256 values simultaneously when in superposition. Quantum logic gates, also in superposition, allow the computer to perform all 256 calculations simultaneously in the time it takes to do just one.

According to the dictionary of quantum mechanics, *Q is for Quantum* by John Gribbin, when the machine enters superposition it behaves like a bunch of computers running in parallel. But we don't know where these other machines are. One seemingly outlandish explanation is that they might exist in parallel universes. In each, the computer processes one of the possible values.

To most people, this 'many worlds interpretation' (MWI) of quantum mechanics is very odd. According to the *Stanford Encyclopedia of Philosophy*, "the MWI is not the most accepted interpretation of quantum theory among physicists". The MWI is just one of several ideas about how the quantum world works.

The late Professor Richard Feynman, recipient of a Nobel Prize for physics and the first to describe a quantum computer, once summed up the bewilderment many feel when confronted with the idea of superposition by saying, "I think I can safely say that nobody understands quantum mechanics".

BEYOND UNDERSTANDING

Confusion apart, there are many possibilities for such a quantum computer. One use for this strange ability lies in solving problems where there's no choice but to work through a large number of solutions looking for the correct one. Problems where we must run an algorithm repeatedly against a long list of combinations of data are common and can take an unfeasibly long time to solve, even using the fastest of today's supercomputing clusters.

Modern cryptographic techniques, for instance, rely on randomly generated, very large prime numbers (upwards of 300 digits) that would take centuries to find by working through a long sequence of numbers and testing each in turn. But according to theory, a quantum computer could try all the numbers simultaneously if we configure the quantum logic gates to represent the desired algorithm, and then set it in superposition. This seemingly magical state then ensures that our quantum computer tests all possible inputs in one

first megabit RAM chip, with over a million on-chip components, became commercially available.

To create today's chips, manufacturers use a technique called lithography. This uses light to etch components on specially prepared silicon. Using shorter wavelengths means that chips can contain more and smaller components. Some manufacturers are now using ultraviolet light of even shorter wavelengths to etch transistors measuring less than 100 nanometres – that's ten thousand transistors per millimetre of silicon.

Transistor counts for individual microprocessors are now in the tens of millions. Some Pentium 4s contain around 55 million, for

instance. Ever-increasing transistor densities present unique problems, however. Transistors generate heat as they work. The more transistors, the more heat is generated. Dealing with this heat is difficult in itself. A more fundamental problem is that the tracks forming connections between components are now only about 25 atoms apart. At this scale, electrons can jump easily between tracks, creating malfunctions.

FINGER ON THE PULSES

In 1996, Neil Gershenfeld and Isaac Chuang of MIT, along with Mark Kubinec of the University of California at Berkeley, built a simple 2-qubit device using molecules of chloroform as the qubits. They precisely focused radio frequency pulses to manipulate them into superposition and arranged other atoms into quantum logic gates to perform calculations. Their delicate device ran Grover's Algorithm (http://en.wikipedia.org/wiki/grover%27s_algorithm), a highly efficient search method designed specifically for quantum computers.

To help make silicon go faster and avoid the problem of jumping electrons, new techniques have emerged. One is strained silicon. This makes transistors switch more efficiently and helps minimise the problem of electrons jumping

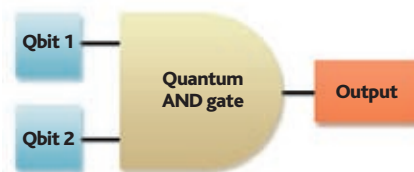
unexpectedly. During manufacture, a heating process stretches the crystalline structure of the silicon in the direction of desired current flow and compresses it in others. Once cooled, electrons find it easier to go where they're supposed to and harder to jump. Strained silicon already finds uses in Intel's Centrino processor. IBM says the technique will enable it to extract up to 20 per cent more performance from its processor ranges.

One day these problems will become insurmountable, though. Hopefully, current research into quantum computing technologies will see hybrid systems with quantum coprocessors appear before silicon has its chips.

THE QUANTUM PROCESSOR

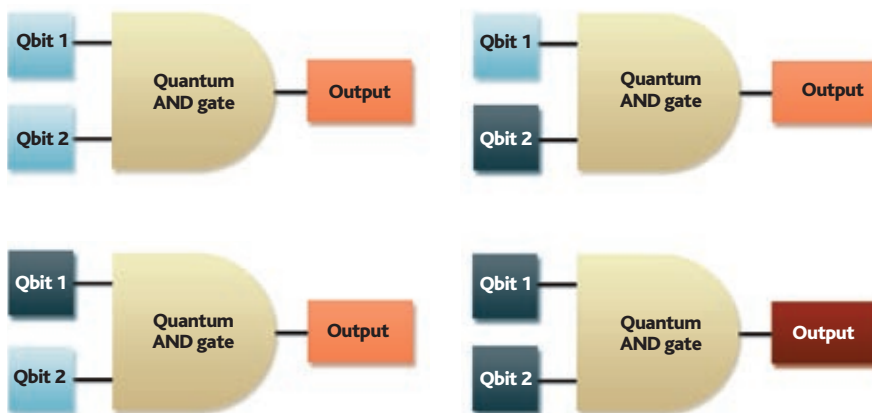
A SIMPLE PROCESSOR

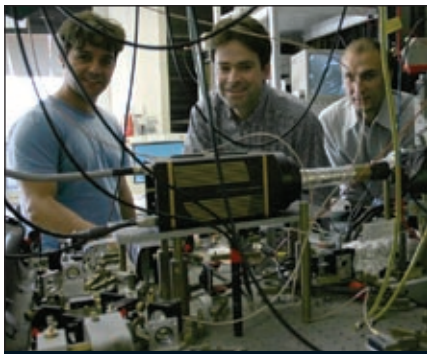
This device consists of a quantum AND gate that outputs a 1 only if both qubits are 1 – otherwise, 0 is outputted. There are four possible combinations of binary inputs, but only one that produces a 1 output.



THE DEVICE IN SUPERPOSITION

When placed in superposition, the quantum processor in effect acts like four machines, each processing one combination of qubits in parallel. Four different outputs appear to coexist.





The University of Bonn team pictured with their five-bit quantum register. Picture courtesy of University of Bonn/Frank Luerweg

perspective, expressed in decimals it would have around 308 digits. Many experimental qbits have decoherence times of around one microsecond, a thousandth of what's required to factorise such numbers. We must calculate how much extra energy we need to spin our quantum pennies for longer.

"If you have decoherence times of over a millisecond, then there is no problem at all," said Gea-Banacloche, "but if the system you are working on has an intrinsic decoherence time of less than a microsecond, then it is more or less hopeless that you will ever be able scale up that system."

Gea-Banacloche has calculated that the smaller a qbit's decoherence time, the larger the amount of energy required to increase the time it stays in superposition. So a qbit with a decoherence time of a second would need just 10 milliwatts of extra energy to double its superposition time, whereas one with a decoherence time of 10 microseconds requires 100 megawatts.

The most efficient way around this is error correction, but Gea-Banacloche isn't too confident about this: "In practice, error correction is what a quantum computer will be doing most of the time." This would make computers based on today's qbit experiments forever limited in their abilities.

BRIGHT HOPES

However, it's possible that Gea-Banacloche is being overly cautious in his scepticism. In 1998, Dr Bruce Kane of the University of Maryland first had the idea of using single phosphorous atoms as qbits. He found phosphorous possesses an unusually long decoherence time of just over half a millisecond.

Though getting nearer a working device, Kane is still cautious about the problems that must be solved along the way. "The dream of a large-scale quantum computer," he said in a paper presented to the US National Academy of Sciences, "will require that engineers overcome the daunting challenge of combining the precision of an atomic clock with the complexity of a modern microprocessor." Despite this advice, some researchers believe they have the necessary mix of skills to build a large-scale quantum processor.

One problem until now has been how to position qbits precisely enough, and observe the results of the calculations they perform. Robert Clark, professor of experimental physics at the University of New South Wales, may have an answer. In 2002, his team conducted an experiment in which they managed to put single phosphorus atoms into specially made holes in an atomically smooth piece of silicon, and then managed to read their spins using a sensitive transistor based on a

POTENTIAL APPLICATIONS

Some problems are impossible to solve without the strange properties and abilities of quantum computers. But while the solutions to some problems may benefit humanity, some could have potentially sinister overtones.

Secure data transmission is an application for quantum computing that's already available in commercial products. To transmit data securely, physicists use a strange property of the quantum world called entanglement to transmit the state of one qbit to another some distance away. An attempt to tap into such a transmission would corrupt the data stream. At the recent Infosecurity Europe show in London, Geneva-based ID Quantique (www.idquantique.com) announced a quantum encryption system called Vectis designed for governments and banks, which can transmit data securely and reliably for up to 100 kilometres using entanglement.

True quantum computers will excel at almost instantly performing a mathematical operation called factorising on extremely long lists of very large numbers. This ability is essential when trying to crack conventional encryption methods, but it's virtually impossible on conventional computers. In the future, however, non-quantum encryption methods may become as insecure as plain text. The ability to intercept and decrypt emails poses unique privacy worries.

Less controversially, quantum computers will also help solve many other problems in mathematics, physics and chemistry. Some problems have so many possible solutions that finding the right one is beyond the scope of a conventional supercomputer. By placing a quantum computer in its superposition state, it

becomes easy to test massive numbers of possibilities in one step. Some pundits even predict that quantum computers will one day enable us to model the birth, evolution and possibly even the death of the universe in unprecedented detail, but there are also more earthly applications.

Nuclear stockpiles need safety testing from time to time, but there's a ban on exploding warheads to see if the rest of a stockpile still works properly or is in danger of exploding randomly in its silo. The only method of testing is to simulate the state of the warheads in software. The calculations required to create a basic simulation require large amounts of supercomputer time. Quantum computers could help minimise the threat of a nuclear accident by peering far into the future of highly detailed simulations.

Another touted use for quantum computers is military and criminal intelligence processing. Finding carefully hidden connections between seemingly random events is computationally intense, but quantum algorithms for searching databases already exist and are waiting for appropriate hardware designs.

The Holy Grail of artificial intelligence is to create a system that can carry out such tasks as a human might. Some consider this impossible without a quantum computer. In their book *Artificial Intelligence: A Modern Approach*, Stuart Russell and Peter Norvig speculate that the human brain's problem-solving ability might actually involve a brute force approach. This is something for which we simply don't have the computing power today, but that quantum computers will be able to do with ease.

single electron. "This was thought to be impossible just a few years ago," he said.

Clark now believes he can also increase the decoherence times of his phosphorus atoms without requiring massive amounts of extra energy, and he hopes to have a chip capable of useful calculations by 2007. "The actual working part of the quantum computer will be measured in billionths of a metre," he said. "But the chip which you basically have to assemble, all the ancillary hardware on there to control readout, error correction... you know that's going to be millimetre-type size by the time we've got all of that onboard."

Late last year came another breakthrough, this time from the Institute for Applied Physics at the University of Bonn. The institute's quantum register uses caesium atoms cooled to a standstill, and holds up to five qbits in a stable, isolated state on the beams of two lasers. A computer-controlled microwave transmitter then sets the spin of individual qbits as required. Remarkably, a special digital imaging camera enabled the team to read the spins on the qbits from the patterns of fluorescent light they created. Long, stable registers are essential to further developments, making this a major advance.

The next step, according to team member Dominik Schrader, is to create programmable

quantum gates that can perform calculations on two or more of the qbits. But the question is, how long will it be before we see a large-scale quantum computer running in the lab? "We hope to get there in two years," said Schrader. "Mind you, in a field like this, you repeatedly come across difficulties that you would not previously have anticipated."

QUANTUM INSIDE

If the various researchers prove Gea-Banacloche wrong and produce useful devices that don't require massive amounts of power, it will be just a matter of time before techniques for commercial quantum processor fabrication follow. There are several alternative approaches left to try even if current approaches fail, too. IBM, for instance, has its own nuclear magnetic resonance technique for setting qbits into superposition and reading their state after calculations are complete. Microsoft also has researchers, such as 1986 Fields Prize recipient Dr Michael Freedman, actively investigating problems in quantum computing.

Whatever the capabilities of the first quantum computers when they finally arrive, one thing remains certain: the speed at which researchers are overcoming the associated engineering obstacles seems to be increasing. At this rate, we might even see 'Quantum Inside' stickers appearing on PCs by the end of the decade. 